(Jr. 1999) (State 2002)REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY) (27-10-2010)	2. REPORT TYPE FINAL	3. DATES COVERED (From - To)

4. TITLE AND SUBTITLE _Deception Recognition: Rethinking the Operational Commander's Approach_	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S) **Mr. Denver E. McPherson, CIV, DOD** Paper Advisor: Captain Michael Fitzpatrick, USN	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The United States today is generally seen as the predominant world superpower because of its economic, political, and military might. Consequently any state or non-state actor at odds with United States policy or strategy is likely to plan and utilize deception as part of an asymmetrical approach to conflict or manipulation against the operational commander. How the operational commander plans for it, and protects against it, should be paramount in the day-to-day implementation of the theater commanders' strategy.

This paper explores the operational commander's vulnerability to this threat. It will define the scope of deception as it is understood today and will identify weaknesses in military deception doctrine and theory. It will explore current counterdeception theory and practice and discuss potential counterarguments that may be made. Finally, the paper draws conclusions concerning the recognition of adversary deception as a critical component of military deception practice and implementation and how it should be operationally addressed.

15. SUBJECT TERMS
Deception, counterdeception, counter-deception, deception recognition, foreign deception, military deception, MILDEC, adversary deception, deception and denial

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Chairman, JMO Dept
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED		24	19b. TELEPHONE NUMBER (include area code) 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Deception Recognition: Rethinking the Operational Commander's Approach.

by

Denver E. McPherson

Civilian, Department of Defense

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the
requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily
endorsed by the Naval War College or the Department of the Navy.

Signature: _____

27 October 2010

Contents

Abstract

The United States today is generally seen as the predominant world superpower because of its economic, political, and military might. Consequently any state or non-state actor at odds with United States policy or strategy is likely to plan and utilize deception as part of an asymmetrical approach to conflict or manipulation against the operational commander. How the operational commander plans for it, and protects against it, should be paramount in the day-to-day implementation of the theater commanders' strategy.

This paper explores the operational commander's vulnerability to this threat. It will define the scope of deception as it is understood today and will identify weaknesses in military deception doctrine and theory. It will explore current counterdeception theory and practice and discuss potential counterarguments that may be made. Finally, the paper draws conclusions concerning the recognition of adversary deception as a critical component of military deception practice and implementation and how it should be operationally addressed.

INTRODUCTION

―Though fraud in other activities may be detestable, in the management of war it is laudable and glorious, and he who overcomes the enemy by fraud is as much to be praised as he who does so by force." -Niccolo Machiavelli, *Arte Della Guerra*

Deception planning and execution is a critical function within the operational art of warfare and has been used effectively by commanders for centuries. Deception has proven time and again to be an effective force multiplier. There is no shortage of examples of brilliant deception operations of past ages. Making an argument for deception and deception planning is rather straightforward. Deception is applied by state and non-state actors, and the level of sophistication is not directly correlated to size, gross domestic product or maturity of actor. Much has been written, studied, practiced, documented, and taught on how to plan deception or make it, but, with the growing importance of deception in the contemporary operating environment, it is at least as critical to examine how to detect deception or break it[1] – and here, past research and practice offers much less guidance. ―All states are vulnerable to deception, including even those whose officials are sophisticated practitioners of the art themselves."[2]

The operational level commander is vulnerable to adversary deception and should formalize an internal systemic deception recognition process. The United States (U.S.) has, in fact, planned and used military deception (MILDEC) throughout its history, and yet in many ways this has rendered it more vulnerable to having deception used against it as well. Planning and conducting MILDEC is typically classified and, in many cases, compartmentalized while limiting participation of planners and decision makers. Consequently, it is an element in the art of war that usually gets little academic attention or rigor simply because most relevant material cannot be obtained by researchers or debated in

open publications. This paper will initially leverage analytic theory and doctrine while fully taking into account that ―theory is an academic term not much in vogue in the Intelligence Community, but it is unavoidable in any discussion of analytical judgment,‖[3] and counterdeception in particular.

Considering there is a plethora written about deception and its history, in addressing this, there will be only a brief review of past experience. This paper will also focus upon historical precedents where they reveal principles affecting deception‗s use by and against the United States in the contemporary setting. Next, this paper will identify where deception recognition and understanding falls short in academia as well as doctrine. Recommendations will then be offered on how the operational commander might address this threat in a systemic way through structure and analytical processes.

CONTEMPORARY EXAMPLES OF DECEPTION

Deception has been around as long as warfare itself. In fact, ―deception must be seen as an accepted and integral part of every military commander‗s repertoire.‖[4] Deception is practiced in many ways. Political deception is overtly recognized and is almost an acceptable practice in the geopolitical landscape. Although, the political environment is subject to its own ―norms of behavior and morality,‖[5] the operational commander can be and usually is directly affected by both political deception and MILDEC and must be able to recognize and respond to each as a matter of course. MILDEC is found throughout all levels of war, strategic through tactical, and is less understood and recognized the more strategic it comes. This analysis will focus only on MILDEC at the operational level while understanding that political, strategic, and operational deception can easily overlap as in a tri-level Venn diagram. Each usually has a cause related to, or effect on the other.

2

The following two contemporary examples of deception reinforce the assertion that the threat of deception is real and establishes the value of understanding how to both use and protect against it. In the first example Saddam Hussein used deception to hold the world at bay and intimidate his neighbors, which ultimately resulted in the invasion of his country. On September 12th, 2002 the White House released a paper entitled ―a Decade of Deception and Defiance: Saddam Hussein‗s Defiance of the United Nations.‖[6] In this document, the UNITED STATES contended that Saddam Hussein violated over 16 United Nations (UN) resolutions in the preceding decade including the ―development of Weapons of Mass Destruction including Biological Weapons, Chemical Weapons, and Nuclear Weapons.‖[7] Further, the document cites several examples of Iraqi defectors admitting to Iraq‗s production of biological agents, and secret facilities set up for the production of chemical, biological, and nuclear weapons.[8] All of these deceptive measures were eagerly accepted by senior U.S. authorities as the catalyst for war. On March 21st, 2003, the United States, along with the United Kingdom, Australia, and Poland, invaded Iraq under the sovereignty of UN resolution 1441.[9] After the invasion and subsequent capture of the Iraqi leader, he was interrogated for months during which he admitted that, in June 2000, he deceived the world in a speech he gave concerning Weapons of Mass Destruction (WMD). He told his interrogator that most of the WMD in his country had been destroyed by UN inspectors during the 1990s and the WMD which had not been destroyed by the inspectors had been dismantled by Iraq itself. When asked why he kept this a secret, Hussein replied that it was very important for him to project that he had WMD to ensure he stayed in power. Doing so ensured the Iranians were not emboldened to attack and prevented them from invading Iraq.[10]

The next example continues along this same storyline. In an uncommon level of openness, General Tommy Franks, in his book *American Soldier*, chronicles how he used deception during the invasion of Iraq in Operation Iraqi Freedom. Even before the first kinetic phase of the war began, he describes how he fed disinformation to the Iraqi intelligence directorate the *Mukhabarat*. In this deception operation, ―which was so sensitive that only a few of us in the U.S. government were aware of it,‖[11] he chronicled how an American military officer code named ―April Fool‖[12] was recruited by the *Mukhabarat* and subsequently doubled back as an agent of the U.S. intelligence apparatus. General Franks describes how his CENTCOM deception cell developed documents marked Top Secret/Polo Step and used these documents to create doubt among Iraq‛s leadership as to ―where, when, and with what size force the coalition would launch its attack.‖[13] The result was Iraq‛s decision to keep the Republican Guard and regular army division‛s in place and focused toward the north as UNITED STATES and coalition forces were building up and subsequently attacking from the south.[14]

Clearly, Saddam Hussein and General Franks knew that deception was an integral part of the art of war. Saddam Hussein used deception to prevent conflict with Iran but ended up provoking invasion by the United States and coalition forces. General Franks used deception to prosecute successful operational level combat operations. The lesson here is that both were successful in making deception, but in the end, warfare might have been prevented if counterdeception recognition cells were dedicated toward systemically watching for deception by Hussein. It is safe to assume that there were few, if any, specially trained strategic or operational counterdeception recognition cells systematically and specifically

looking for deception to ensure that the operational commander and strategic leadership understood exactly what they were up against. The question is why not?

UNDERSTANDING DECEPTION PLANNING

To some degree, planning for a deception operation is different than any of the other operational planning processes. Deception recognition will generally be accomplished with a much smaller team, who must understand both the friendly operational plan and the nature of any adversary vulnerabilities the deception might effectively target. To do this, it takes the talented efforts of operational and intelligence planners in close concert with each other to make sure that the intended deception is believable.

A deception story must embody four characteristics to be successful. It must be believable, verifiable, consistent, and executable.[15] Failing on any of these dimensions means that the plan will most likely fall short of its objective. With this in mind, deception planning should progress along the four steps of See, Think, Do,[16] and Goal. *See* is identifying the observables, the events and actions and means in which to reach the target. *Think* is the story: the perception we want our target to have. *Do* is the reaction or objective of the story. *Goal* is the end state desired: what decision or action does the planner want the decision maker to make?[17]

Joint doctrine effectively directs MILDEC as a function in the operational planning process. Understanding deception is important enough to be established in policy in the form of JP 3-13.4 (Military Deception), which defines MILDEC as ―those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."[18] In providing guidance in

MILDEC planning, joint doctrine dictates that the commander must adhere to six basic principles:

- **FOCUS –** Target the adversary decision maker

- **OBJECTIVE –** cause an adversary to take or not to take specific action

- **CENTRALIZED PLANNING AND CONTROL –** self-explanatory

- **SECURITY –** deny adversary knowledge of the friendly plan

- **TIMELINESS –** carefully timed for when it is likely to have maximum impact in distracting the adversary from the friendly plan

- **INTEGRATION –** full integration with the operational planning, especially to divert adversary attention at decisive points in the friendly plan[19]

Planning MILDEC is not an amateur sport. Joint doctrine dictates that MILDEC planners should be specifically trained to accomplish this planning.[20] If a MILDEC operation was to be detected by the adversary it could easily result in counterdeception operations being conducted against the operational commander, potentially ending with disastrous results.

COUNTERDECEPTION ANALYTIC TAXONOMY

Counterdeception includes the detection of deception.[21] This is accomplished through a series of steps by individuals who not only intimately understand their target but also have a deeper understanding of themselves and how they think. Being able to predict deception early on, or as it is happening, would be the equivalent of an intelligence coup d'état within the analytical process. This rarely happens. Yet, many dedicate their life's work toward this goal. Having the experience and training to do this is the difference between an average analyst and a great analyst. To be at the top of the analytical game, one

would have the ability to minimize cognitive bias or pre-conception, identify the potential deception and see the situation as it relates to the target. This is the terribly complex and difficult part of counterdeception and is most likely why many shy away from its theory and practice. This is also why much of this paper will be spent on dissecting the characteristics of counterdeception analysis in order to validate why the operational commander's counterdeception cell must be specifically trained and systemically focused toward their target.

To understand your enemy is to understand his culture. ―To wage war, become an anthropologist. Lose the fascination with Clausewitz, and embrace culture as the way to understand conflict. Or so argue a number of strategists, historians, and officers on both sides of the Atlantic."[22] In this statement, Patrick Porter is emphasizing that different countries and cultures invariably have different norms and mores, and ways of looking at the world, and to know this is to win at war. This is also fundamental to understanding adversary deception. A culture's norms will dictate its appropriate and inappropriate values, beliefs, attitudes and behaviors. Understanding this cultural relativism gives us insight into intent. Social norms tend to be tacitly established and maintained through body language and non-verbal communication between people in their normal social discourse. This will have a cause and effect on both the part of the analyst's perception and the intent of an adversary in the course of deception activity.

Because other countries and cultures have dramatically different norms than ours, cognitive analysis, as it relates to deception, must be approached with a clear understanding of both the adversary's norms and one's own. Cognitive bias, read norms, will often have as

much influence on the analyst's perception of the target as the information collected on the target itself.

As an example, to understand the People's Republic of China intent one must understand that Chinese preferences and prejudices are much different than in the western culture. In the Chinese culture, people respond to *Guanxi*, which is to establish an overt social relationship, before conducting business. Americans typically bypass the concept of *Guanxi*, and consider it an impediment to business. In another example, the concept of ―face‖ in dealing with people in a personal or professional relationship is first and foremost in the Chinese culture. The western analyst should be aware that to dishonor one's self or family is far more of a concern in the Chinese culture than to lie to an individual or business entity. In western society, which has its roots in Judea Christian beliefs, people are motivated by guilt. Therefore, westerners have a hard time reconciling that lying to save honor is not wrong.

Counterdeception analysts should understand themselves as well as they understand the enemy. Richard Heuer's fundamental study of the epistemological question, ―What is truth and how can we know it?‖ is the foundation for his theory and writings about cognitive challenges in intelligence analysis. His findings are applicable in the study of the cognitive challenges and appropriate for a counterdeception analyst to consider when dealing with, or identifying, a deceptive threat against the operational commander. His theory of cognitive (judgmental) bias is not based on analytical incompetence or laziness by the analyst, but a subconscious human mental procedure for processing information. Look at it as a thinking error, which distorts the analyst's evaluation of evidence, in some cases even after that evidence has been discredited. Heuer asserts that because humans are predisposed to bias,

analysts often ―reject the possibility of deception because they see no evidence of it.‖[23] He further states ―that the possibility of deception should not be rejected until it is disproved or, at least, until a systematic search for evidence has been made and none has been found.‖ [24]

What we see from this argument is that there is an innate or inborn predisposition to the way an analyst will process information and develop a hypothesis, and that one does not have the ability to completely separate this predisposition (and cultural influences) from ―objective‖ knowledge of the world acquired through past experience. In other words, everyone is a prisoner of their own history. Considering this, we can argue that in order to fully understand the meaning of information or messages as they are intended to be received, those within a counterdeception cell should be trained in the ability to consciously recognize and compensate for, to any extent possible, these learned experiences and influences.

The inability to set biases aside, resulting in analytical faux pas like mirror imaging,[25] is a human characteristic affecting analysts. Richard Heuer offers a potential solution for this dilemma. He argues that tools and techniques that gear the analyst‗s mind toward applying higher levels of critical thinking would substantially improve analysis on complex issues such as deception analysis. One of these tools, which has been described as one of Richard Heur‗s ―most important contributions,‖[26] is Analysis of Competing Hypothesis (ACH).[27] Simply put, ACH is a technique used to challenge and compete, against each other, a series of plausible hypothesis to see which one is least incompatible with available information. A detailed discussion of ACH is beyond the scope of this paper but suffice it to say there is hope for the counterdeception analyst!

Identifying potential adversary deception requires a structured cognitive process not typically exercised today. This is referred to as the Deception Analysis Cognitive Process

(DACP).[28] The explicit reference to analysis is most likely the reason the commander and

his J3 typically defer to the J-2 as the lead. This is problematic for many reasons. Deception

planners are typically a cell of operational, planning, and intelligence personnel. The

deception planning skills are the foundation on which a second cell of similar composition,

augmented with specialized counterdeception training, would need to build upon to

successfully apply the DACP. Currently, the DACP is broken down into eight separate

phases: Recognition, Evaluation, Emulation, Selection, Implementation, Collection,

Integration, and Resolution (REESICIR).[29] This process has been used at the strategic level

with success. It should be one of the central processes an operational commander would

expect from his counterdeception cell. Recognizing Richard Heuer's assertions that all

analysts bring intrinsic biases to the table, the DACP will help mitigate this to some extent.

The use of these phases tailored for the counterdeception cell might appear as follows:

> **RECOGNITION:** The counterdeception cell must recognize what to look for. This
>
> can be self-initiated by observing anomalies or understanding the targets historical
>
> predisposition to using deception. Requirements can also come from higher HQ's or
>
> as a result of cross-cueing by other intelligence sources.
>
> **EVALUATION:** This is a thorough evaluation of not only the target but also a
>
> review of the counterdeception cell member's vulnerabilities (biases). An evaluation
>
> of the target should contain an analysis of whether it is plausible and feasible for the
>
> target to conduct deception and to what extent. Is it plausible, or has the target done
>
> this before?
>
> **EMULATION:** This is the question of identifying or recognizing how the threat will
>
> conduct deception. A study of the deceptive events that led up to the 1973 Yom

Kippur War, or deceptive actions taken by India prior to its nuclear test detonations in 1998, which caught most of the world by surprise, would show us that identifying deception is more than seeing one anomaly or act. A counterdeception cell must be expert in the target country's history, culture, and likely future intent.

SELECTION: This refers to choosing the approach by which the counterdeception cell would identify activities of deception. This is where sophisticated analytical skills and use of tools is critical. There are many different processes one might use. We have already identified ACH as one such tool.

IMPLEMENTATION: This is self-explanatory. It is implementing the process that the counterdeception cell has chosen. If the cell chooses to use ACH then it would implement the 8 steps involved.[30]

COLLECTION: This includes the identification of tools like the Tripwire Analytic Capability (TAC) program (an unclassified system) already used by intelligence analytic teams at all levels. The TAC system allows the cell to develop very sophisticated inquiries into anomalies of current and historical information. Then the cell might develop a collection strategy to fill gaps, or resolve anomalies.

INTEGRATION: This is the assimilation of the information from the collection plan and other tools to begin the formulation of a hypothesis or recommendation. Integrating the information will give the counterdeception cell a more refined picture of what it is seeing. As well, it will give it a better foundation to develop its hypothesis and eventually its recommendation.

RESOLUTION: This is the culmination of the DACP. The cell will make a determination at this point of whether the target is highly likely, likely, or not likely to be conducting deception.

Having the right team, properly trained, and specifically looking for adversary deception will give the operational commander a significant advantage in identifying deception against his command's mission. So why isn't this team a regular part of the commands structure and mission?

JOINT DOCTRINE ON OPERATIONAL DECEPTION

Joint doctrine is the cornerstone used by operational commanders when organizing and managing their commands, yet is used sparingly when addressing the complex phenomena of counterdeception. Joint Publication (JP) 3-0 (Joint Operations) doesn't mention deception operations. JP 3-13 (Information Operations) describes MILDEC as a core capability of the Information Operations (IO) program and posits that it is fundamental to the success of the IO program. It briefly describes MILDEC from the operational perspective in how it should be coordinated and complement the Operational Security Plan. It states that ―MILDEC planning and oversight responsibility is normally organized as a staff deception element in the operational directorate (J-3).‖[31] It does reference JP 3-58 (Joint Doctrine for Military Deception) for further discussion. JP 3-58 has subsequently been replaced by JP 3-13.4 (Military Deception). JP 3-13.4 discusses in great detail how to plan and execute deception from a military point of view but falls short of adequately helping the operational commander understand how to protect against adversary deception operations. It addresses counterdeception as an element of MILDEC. Its primary assertion is that

―countering deception is difficult. Knowing deception methods an adversary has used successfully is important."[32] Oddly, the follow-on discussion about counterdeception focuses on what to do *after* a deception operation is revealed. It is interesting to note that all of this discussion is under the paragraph labeled ―Detection of Adversary Deception,"[33] yet there is no discussion concerning *how to detect* adversary deception. JP 5-0 (Joint Operation Planning) does not discuss or mention deception planning at all. Milan N. Vego, considered one of the foremost scholars of Joint Operational Warfare, discusses in great detail in his book *Joint Operational Warfare; Theory and Practice* operational/strategic deception and how to make it but provides no insight into how to protect against it, or break it. Doctrine and academia present adequate insight into planning for deception but fall considerably short in addressing the detection of adversary deception. There is no standardized guidance or frame of reference for the operational commander and his staff to adequately address this potential threat. Consequently, commanders and their staffs are left to their own devices to determine if and when adversary deception operations are being conducted against them.

Breaking it, or recognizing adversary deception, has typically been relegated to chance, with the operational commander deferring to the Director of Intelligence (J-2) and his analysts to identify adversary deception in the normal course of their running analytical review of the operational environment. This is problematic, since most, if not all, operational-level J-2 analysts lack training in the cognitive analytical techniques needed to adequately recognize deception directed against the operational commander. Yet, the threat is real, it is in many cases sophisticated, and it is ongoing. Failing to recognize this and protect against it is to assume significant risk to current and future operations by leaving the operational commander vulnerable to adversary deception.

ANALYSIS AND RECOMMENDATIONS

One might argue that J-2 analysts are the most appropriate tool the commander has in recognizing this threat, as superficially alluded to in JP 3-13.4. This argument places too much confidence in a typically undertrained, overburdened group and oversimplifies the techniques involved and the metacognition[34] skills required to identify this type of threat. Recognizing adversary deception requires a cell of focused analysts who are specifically trained in the fundamental techniques of deception analysis. Richards Heuer, universally recognized as one of the leading authorities in the psychology of intelligence analysis and denial & deception theory, makes three fundamental observations reinforcing this. He asserts that the mind is poorly wired for effectively dealing with inherent uncertainty and induced uncertainty; increased awareness of cognitive bias does little to deal effectively with uncertainty; and techniques in assisting the analyst in applying a higher level of critical thinking will substantially improve the analytical ability to deal with complex issues when faced with information that is incomplete, ambiguous, and many times deliberately distorted.[35]

A typical active duty military intelligence analyst within the operational command is not usually given the opportunity to study and analyze a targeted adversary for more than a three year assignment. During this tour, this analyst might receive specialized formal instruction in basic analysis techniques such as storyboarding etc. In some cases, this analyst might be lucky enough to be assigned to a counterintelligence or counterterrorism section and be given more analytical training geared toward a specific discipline. In rare circumstances will the organization allow the time for an analyst to step away from his already substantial day-to-day duties to study denial and deception analytical techniques.

Basic analytical training is usually adequate to support the day to day understanding of the conventional threat within the theater of operations but is inadequate when facing a more complex threat such as deception. It is generally accepted among professional intelligence agencies, civilian and military, that to become an effective general analyst one should study the target for a minimum of three years.[36]

To adequately address the deception threat, the commander should have a cell of experts dedicated to looking at this problem set. This organic cell wouldn't need to be large, but should consist of one or two trained target intelligence analyst's, one operational (non-intel) member and a Directorate of Plans (J5) planner who is familiar with the command's operational plan directed at the adversary. This cell would need to work together as a long-term systemic team that has been specifically trained in deception analysis. A counterargument would be of course that this is simply too taxing on an already understaffed and overburdened command. This is an understandable perspective. Yet, consider the operational staff deception element mentioned in JP 3-13 or the CENTCOM operational deception cell mentioned by General Franks in his book. If it is important enough to dedicate assets to plan and manage the execution of deception, it certainly would be just as important to have a cell of experts to ensure protection against it.

Not every operational commander will need a cell focused on potential adversary deception. In an ideal world, there would be such a cell in every Combatant Command headquarters or staff. Although, if the command decides that it cannot afford to devote the bodies, it might be facing too much risk if they are not addressing one of these known deception practitioner's such as Pacific Command (PACOM) for North Korea, and China, European Command (EUCOM) facing Russia, and Central Command (CENTCOM) dealing

with Iran, and non-state actors such as Al Qaida, certainly should consider dedicated adversary counterdeception cells within their commands.

An effective cell brought together to identify adversary deception should be drawn from individuals who already understand how to operationally plan deception. It is important to emphasis that the skills in planning for deception are not synonymous with the skills needed in how to recognize it. There is no known correlation between being good at planning deception and being good at analyzing deception. The challenge will be in finding individuals who have been trained in the fundamentals of recognizing it. Where this cell resides is not as important as the task it will face. Depending on the commander's established area of operations, the J-2 will structure his Joint Intelligence Center (JIC) by regional teams or country teams. There is no patent solution since every command dynamic is different. Having a dedicated, well-trained counterdeception analytical cell is the key for the operational commander to protect against adversary deception. This team would fit fine in either the J-2's JIC or within an operational cell within the J-3.

Although the focus of this paper is on the operational commander addressing this threat organically, it is appropriate to mention that it would be unreasonable for him to be able to expect this cell to work in a vacuum and still be successful. In other words, this cell will need dedicated strategic counterdeception support. Although not within the scope of this paper, there are many defense agencies and interagency organizations that should consider like type cells and processes which would be in direct support of a specific theatre commander.

CONCLUSIONS

For the operational commander to minimize risk in all phases of war he must be comfortable that the decisions he makes are based on a clear, true, unambiguous understanding of his adversary to the maximum extent possible. He must feel comfortable that the decisions he makes are not a result of adversary deception influencing his actions. As we have seen, this could be the difference in whether a nation goes to war or not -- and if so, could mean the difference between success and failure.

To ensure the recognition of deception is adequately addressed, he should have a group of dedicated, well-trained personnel who understand not only the adversary but ensure that their own cognitive bias and ambiguity are minimized. We have seen that this does not take a large group, but a small, focused effort from the intelligence, operational, and planning directorates. This cell must train, and work together on a systemic basis ensuring that the whole is truly greater than the sum of its parts.

This cell must understand how to plan deception but only to the extent in which to provide a foundation for understanding how to facilitate their identifying and breaking an adversarial deception plan. This cell should be solely dedicated toward counterdeception activities.

This cell should be specifically trained in cognitive counterdeception techniques to have insight in cognitive bias, mirror imaging, ACH and REECISER. This will give them the tools that will enable them to successfully carry out their critical mission.

NOTES

[1] As taught by the National Defense Intelligence College (NDIC), Denial & Deception Advanced Studies Program (DDASP), Making it and Breaking it are teaching concepts which discuss the art of planning deception and recognizing deception.

[2] Cynthia M. Grabo, *Anticipating Surprise; Analysis for Strategic Warning* (Washington, DC: Joint Military Intelligence College's Center for Strategic Intelligence Research, 2002), 129.

[3] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the study of Intelligence CIA, 1999), 34.

[4] Michael I. Handel, ―Military Deception in Peace and War," Jerusalem Papers on Peace Problems 38 (1985), 7.

[5] Ibid., 7.

[6] America.gov, ―A Decade of Deception and Defiance," *Department of State; Office of International Information Programs,* http://www.america.gov/st/washfile-english/2002/September/20020912121332ljbrown@pd.state.gov0.751034.html *(accessed 16 October 2010).*

[7] Ibid.

[8] Ibid.

[9] United Nations, Security Council 4644th Meeting (AM), ―Security Council Holds Iraq In ‗Material Breach' Of Disarmament Obligations, Offers Final Chance To Comply," S/Res/1441/2002, http://www.un.org/News/Press/docs/2002/SC7564.doc.htm (accessed 16 October 2010).

[10] Henry Shuster, ―Interrogator Shares Saddam's Confessions," *CBSNEWS.COM*, 27 January 2008, http://www.cbsnews.com/stories/2008/01/24/60minutes/main3749494.shtml (accessed 16 October 2010).

[11] Tommy Franks and Malcolm McConnell, *American Soldier* (New York, NY: HarperCollins Publishers, 2004), 434.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] As taught by the National Defense Intelligence College (NDIC), Denial & Deception Advanced Studies Program (DDASP).

[16] Chairman, U.S. Joint Chiefs of Staff, *Military* Deception, Joint Publication (JP) 3-13.4 (Formerly JP 3-58) (Washington, DC: CJCS, 13 July 2006), IV-1. The noun Goal is added by the author. Goal is taught at the National Defense Intelligence College (NDIC), Denial & Deception Advanced Studies Program (DDASP) and has not been formally incorporated into US Joint Doctrine as of the date of this paper.

[17] As taught by the National Defense Intelligence College (NDIC), Denial & Deception Advanced Studies Program (DDASP).

[18] Chairman, U.S. Joint Chiefs of Staff, *Military Deception*, Joint Publication (JP) 3-13.4 (Formerly JP 3-58) (Washington, DC: CJCS, 13 July 2006), IV-1.

[19] Ibid., viii.

[20] Ibid., x.

[21] John Gooch and Amos Perlmutter, *Military Deception and Strategic Surprise* (London, England: Routledge Taylor and Francis Group, 1982), 190.

[22] Patrick Porter, *Good Anthropology, Bad History: The Cultural Turn in Studying War* (Carlisle, PA: US Army War College Press, 2007),1. http://www.carlisle.army.mil/USAWC/parameters/Articles/07summer/porter.pdf (accessed 3 October 2010).

[23] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the study of Intelligence CIA, 1999), 98.

[24] Ibid, 98.

[25] Ibid, 70. Heur defines mirror imaging as ―One kind of assumption an analyst should always recognize and question is mirror-imaging—filling gaps in the analyst's own knowledge by assuming that the other side is likely to act in a certain way because that is how the US would act under similar circumstances."

[26] Ibid, 95.

[27] Ibid.

[28] As taught by the National Defense Intelligence College (NDIC), Denial & Deception Advanced Studies Program (DDASP).

[29] As taught by the National Defense Intelligence College (NDIC), Denial & Deception Advanced Studies Program (DDASP), REESICIR is an acronym used to describe the deception analysis cognitive process used by analysts in detecting deception.

[30] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the study of Intelligence CIA, 1999), 96.

[31] Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13 (Washington, DC: CJCS, 13 July 2006), II-3.

[32] Chairman, U.S. Joint Chiefs of Staff, *Military Deception*, Joint Publication (JP) 3-13.4 (Formerly JP 3-58) (Washington, DC: CJCS, 13 July 2006), II-1.

[33] Ibid., II-2.

[34] Metacognition as defined by the World English Dictionary is thinking about one's own mental processes. Metacognition is the cornerstone philosophy is training counterdeception techniques and adversary deception recognition.

[35] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the study of Intelligence CIA, 1999), xx.

[36] This theory is a rule of thumb and not a specific requirement for advancement at the Defense Intelligence Agency. Civilian analysts are usually trained in fundamental analytical techniques and generally given two to three years before their analysis of a given target is considered authoritative based on experience and training. Most analysts who are seen as experts have spent years studying their target and training in the nuances of fundamental analysis, not necessarily deception analysis.

BIBLIOGRAPHY

America.gov. "American Government." *A Decade of Deception and Defiance.* September 12, 2002. http://www.america.gov/st/washfile-english/2002/September/200209121332ljbrown@pd.state.gover0.751034.html (accessed 16 October 2010).

Caddell, Joseph W. "Deception 101.*"* Strategic Studies Institute, December 2004, 1-22

Dewar, Michael. *The Art Of Deception In Warfare.* New York, NY: Sterling Publishing Co. Inc., 1989.

Franks, Tommy, and Malcolm McConnell. *American Soldier.* New York, NY: Harper Collins Publishers Inc, 2004.

Gerwehr, Scott and Glenn W. Russell. *The Art of Darkness: Deception and Urban Operations.* Santa Monica, CA: Rand, 2000.

Gilovich, Thomas. *How We Know What Isn't So.* New York, NY: The Free Press, 1991.

Godson, Roy, and James J. Wirz. *Strategic Denial and Deception: The Twenty-First Century Challenge.* Piscataway, NJ: Transaction Publishers, 2002.

Gooch, John, and Amos Perlmutter. *Military Deception and Strategic Suprise.* London, England: Routledge Taylor & Francis Group, 2007.

Grabo, Cynthia M. *Anticipating Suprise; Analysis for Strategic Warning.* Washington, DC: Joint Military Intelligence College, 2002.

Handel, Michael I. "Military Deception in Peace and War." *Jerusalem Papers on Peace Problems*, no.38, (1985): 1-60.

Heuer Jr., Richard J. *Psychology of Intelligence Analysis.* Washington, DC: Central Intelligence Agency, 1999.

Latimer, Jon. *Deception in War: The Art of The Bluff, The Value of Deceit, and the Most Thrilling Episodes of Cunning in Military History, from the Trojan Hourse to the Gulf War.* New York, NY: The Overlook Press, 2001.

Lloyd, Mark. *The Art of Military Deception.* London, England: Leo Cooper, 1997.

Porter, Patrick. *Good Anthropology, Bad History: The Cultural Turn in Studying War.* Carlisle, PA: US Army War College, 2007.

Shuster, Henry. ―Interrogator Shares Saddam‗s Confessions," *CBSNEWS.COM*, 27 January 2008. http://www.cbsnews.com/stories/2008/01/24/60minutes/main3749494.shtml (accessed 16 October 2010).

Smith, Douglas V. *Military Deception and Operational Art.* Occasional Paper, no.14, Newport, RI: US Naval War College, 1993.

United Nations. Security Council 4644th Meeting (AM). ―Security Council Holds Iraq In ‗Material Breach‗ Of Disarmament Obligations, Offers Final Chance To Comply." S/Res/1441/2002. http://www.un.org/News/Press/docs/2002/SC7564.doc.htm (accessed 16 October 2010).

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operations*. Joint Publication (JP) 3.0. Washington, DC: CJCS, 13 February 2006.

―. U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

―. U.S. Office of the Chairman of the Joint Chiefs of Staff. *Military Deception*. Joint Publication (JP) 3-13.4 (Formerly JP 3-58). Washington, DC: CJCS, 13 July 2006.

―. U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint OperationsPlanning*. Joint Publication (JP) 5.0. Washington, DC: CJCS, 26 December 2006.

Vego, Milan N. *Joint Operational Warfare: Theory and Practice.* NewPort, RI: U.S. Naval War College, 2009.